Configuring RADIUS

Router Software Version 11.02
Site Manager Software Version 5.02

Part No. 116752 Rev. A
May 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1997 Bay Networks, Inc.

All rights reserved. Printed in the USA. May 1997.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, Bay Networks, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ARN, ASN, BaySIS, BayStack, BayStream, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Before You Begin xiii
Conventions xiv
Acronyms xv
Ordering Bay Networks Publications xv
Bay Networks Customer Service xvi
How to Get Help xvi
For More Information xvii

Chapter 1
Starting RADIUS

How to Use This Manual 1-1
Before You Begin 1-2
Enabling RADIUS 1-3
Specifying the Client's IP Address 1-8
Specifying the Primary Server's IP Address 1-9
Selecting a Protocol for RADIUS Authentication 1-11

Chapter 2
RADIUS Overview

How RADIUS Works 2-1
Bay Networks RADIUS Implementation 2-2
RADIUS Authentication 2-3
Using PPP for Dial-up Connections 2-3
Using IP and IPX Unnumbered Protocols for PPP Connections 2-4
Configuring the Remote User to Work with the RADIUS Client 2-5
RADIUS Accounting 2-6
Using PPP for Dial-up Connections 2-6
Configuring a Dial Service for RADIUS Accounting 2-6
Using RADIUS-Compatible Servers with the RADIUS Client 2-7

Accepting Remote Users' IP Addresses 2-7
For More Information 2-8

Chapter 3
Customizing the RADIUS Client Configuration

Modifying the Client's IP Address 3-1
Modifying Service from Authentication to Accounting 3-2
Modifying the Protocol for RADIUS Authentication 3-3
Modifying the PPP Authentication Protocol 3-6
Removing RADIUS Authentication and Accounting 3-8

Chapter 4
Customizing the RADIUS Server Configuration

Modifying the Primary Server's Password 4-1
Modifying the Server Mode 4-3
Authentication and Accounting UDP Ports 4-3
Modifying the Server Response Time 4-4
Modifying the Number of Client Requests to the Server 4-4
Configuring Alternate Servers 4-5
Reconnecting to the Primary Server 4-7
Changing the Primary and Alternate Servers 4-7
Removing a Server Entry 4-8

Appendix A
RADIUS Parameters

Client IP Address Parameter A-1
Server Configuration Parameters A-2
Protocol Parameters for RADIUS Authentication A-5

Appendix B
RADIUS Parameter Defaults

Appendix C
Configuration Examples

Configuring RADIUS Authentication C-2
Before You Begin C-2
Enable RADIUS Authentication C-3
Select IP C-4

Configuring RADIUS Accounting C-5
Before You Begin C-6
Create a Backup Pool C-6
Create a Dial Backup Circuit C-7
Enable RADIUS Accounting C-8
Configuring RADIUS Accounting and Authentication C-9
Before You Begin C-10
Enable Dial Backup Service C-10
Enable RADIUS Accounting and Authentication C-10
Select IP for RADIUS Authentication C-11
Index

Figures

Figure 1-1. Configuration Manager Window 1-3
Figure 1-2. RADIUS Client Configuration Window 1-4
Figure 1-3. RADIUS Menu 1-4
Figure 1-4. Choose WAN Serial Interface Type Window 1-5
Figure 1-5. Sync Line Media Type Window 1-6
Figure 1-6. Async Line Media Type Window 1-6
Figure 1-7. ISDN Switch Configuration Window 1-7
Figure 1-8. ISDN Logical Lines Window 1-7
Figure 1-9. Primary Server Address Window 1-9
Figure 1-10. RADIUS Server Configuration Window 1-10
Figure 1-11. RADIUS Dial_In Slot Window 1-11
Figure 1-12. RADIUS Dial_In Protocol Window 1-12
Figure 1-13. Dial Optimized Routing Query Window 1-12
Figure 2-1. Sample Network Using RADIUS 2-2
Figure 3-1. RADIUS Client Configuration Window 3-1
Figure 3-2. RADIUS Dial_In Slot Window 3-3
Figure 3-3. RADIUS Dial_In Protocol Window 3-4
Figure 3-4. Dial Optimized Routing Query Window 3-4
Figure 3-5. PPP Interface List Window 3-6
Figure 3-6. PPP Line Lists Window 3-7
Figure 4-1. RADIUS Server Configuration Window 4-2
Figure 4-2. RADIUS Server Configuration Window 4-5
Figure 4-3. Alternate Server Address Window 4-6
Figure C-1. Sample Network Using RADIUS Authentication C-2
Figure C-2. Sample Network Using RADIUS Accounting C-5
Figure C-3. Sample Network Configured for Dialing an Alternate Site C-9

Tables

Table B-1. RADIUS Parameter Defaults B-1

About This Guide

If you are responsible for configuring Remote Authentication Dial-In User Service (RADIUS) software, read this manual.

If you want to	Go to
Start RADIUS on a router using the parameter defaults	Chapter 1
Learn about RADIUS and the Bay Networks® implementation of RADIUS	Chapter 2
Change parameter defaults for the RADIUS client configuration	Chapter 3
Change parameter defaults for the RADIUS server configuration	Chapter 4
Obtain information about RADIUS parameters (this is the same information you obtain using Site Manager online Help)	Appendix A
Quickly obtain the default value of a RADIUS parameter	Appendix B
See RADIUS configuration examples	Appendix C

Before You Begin

Before using this manual, complete the following tasks. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers*, *Connecting AN and ANH Systems to a Network*, or *Connecting ASN Routers to a Network)*.

Make sure that your router is running the latest version of the Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7–10.xx to Version 11.0*.

Conventions

bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

CHAP	Challenge Handshake Authentication Protocol
IP	Internet Protocol
IPX	Internet Packet Exchange
IPXWAN	Internet Packet Exchange Wide Area Network
ISDN	Integrated Services Digital Network
ISP	Internet service provider
ITU-T	International Telecommunication Union–Telecommunications (formerly CCITT)
LAN	local area network
OSPF	Open Shortest Path First (protocol)
PAP	Password Authentication Protocol
POTS	plain old telephone service
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SAP	Service Advertising Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
WAN	wide area network

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 1-888-422-9773
- Phone--International: 1-510-490-4752
- FAX--U.S./Canada and International: 1-510-498-2609

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	1-800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 1-508-436-8880 (direct)	1-508-670-8766
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	1-800-2LANWAN	508-670-8765
Santa Clara, CA	1-800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

For More Information

For information about Bay Networks and its products, visit the Bay Networks World Wide Web (WWW) site at http://www.baynetworks.com. To learn more about Bay Networks Customer Service, select Customer Service on the opening Web page.

Chapter 1
Starting RADIUS

Remote Authentication Dial-In User Service (RADIUS) defines a method of centralizing authentication and accounting information for networks with many remote dial-in users. By placing authentication and accounting functions in one central location, you can improve security and better manage large networks.

In a network using RADIUS, the router is the RADIUS client. The client is the connection point between remote users and a RADIUS server. The server has the information that it needs to identify remote users and to keep accounting information for each call.

How to Use This Manual

Understanding how this manual is organized should make it more useful to you. The manual is organized as follows:

- Starting RADIUS

  Begin by reading this chapter, which explains how to enable RADIUS on your router using a basic configuration, that is, a configuration that uses all of the available parameter defaults.

- RADIUS overview

  Provides information about RADIUS authentication and accounting and the Bay Networks implementation of these services. This information is in Chapter 2.

- Instructions for modifying the default configuration introduced in Chapter 1

  These instructions are in Chapters 3 and 4. Most of the instructions assume that you have read Chapter 1 and explain how to modify the default configuration.

The steps that instruct you to set a parameter value are followed by a box that includes the Site Manager parameter and the location of the parameter description in Appendix A. To read more about the parameter before setting a value, refer to the specified page. You can also read these parameter descriptions by clicking on Help in the Site Manager windows.

- Parameter descriptions, parameter default tables, and configuration examples

  This information is in Appendixes A through C.

Before You Begin

Before you enable RADIUS, do the following:

1. Create and save a configuration file that has at least one wide area network (WAN) interface.
2. Retrieve the configuration file in local, remote, or dynamic mode.
3. Specify the router hardware if this is a local-mode configuration.
4. Configure the physical interface for any ISDN lines that you will use for RADIUS.

   Refer to *Configuring Dial Services* to learn how to configure ISDN lines.
5. Configure one or more dial services so the RADIUS client can accept calls from the remote user (RADIUS accounting only).

   Configure dial-on-demand, dial backup, or bandwidth-on-demand service to operate with RADIUS accounting. Refer to *Configuring Dial Services* for instructions. Once you enable RADIUS authentication, the RADIUS client automatically configures a dial connection; therefore, you are not required to configure a dial service.
6. Enable dial optimized routing on the remote routers (RADIUS authentication only).

   Dial optimized routing prevents Routing Information Protocol (RIP) updates or Service Advertising Protocol (SAP) updates from keeping a line active unnecessarily, thereby reducing the line costs. Enabling this feature improves the operation of RADIUS authentication.

Enabling RADIUS

To enable RADIUS accounting or authentication, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Create RADIUS (Figure 1-1).**

Figure 1-1. Configuration Manager Window

Site Manager displays the RADIUS Client Configuration window (Figure 1-2), which shows the router slots available for configuring RADIUS.

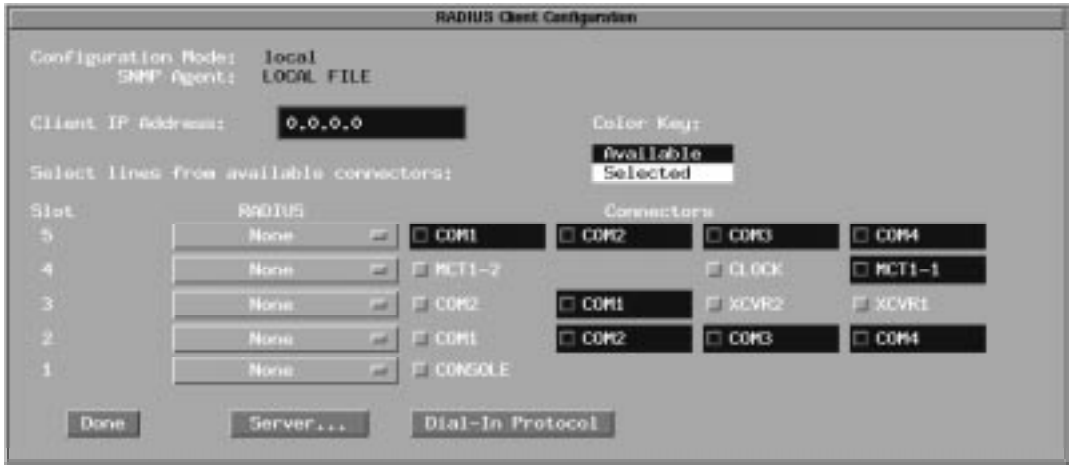

Figure 1-2. RADIUS Client Configuration Window

2. **To configure a slot for RADIUS, click on the box labeled None.**

   Site Manager displays a menu showing the RADIUS options (Figure 1-3).

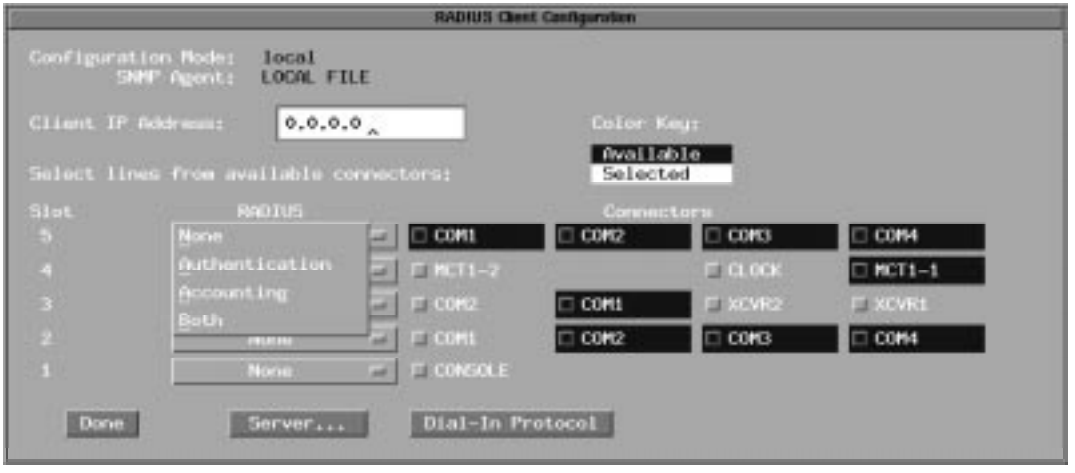

Figure 1-3. RADIUS Menu

3. **Select Authentication, Accounting, or Both to enable both services.**

   If the router is already using a slot for dial-on-demand, dial backup, or bandwidth-on-demand service, you cannot select this slot for authentication. This restriction does not apply to accounting.

4. **For RADIUS authentication, select the connectors that you want to serve as RADIUS interfaces. This is not required for RADIUS accounting.**

   - To configure a modem line for RADIUS, click on a COM connector. (To configure an ISDN line for RADIUS, go to page 1-7.)

     Site Manager displays the Choose WAN Serial Interface Type window (Figure 1-4).

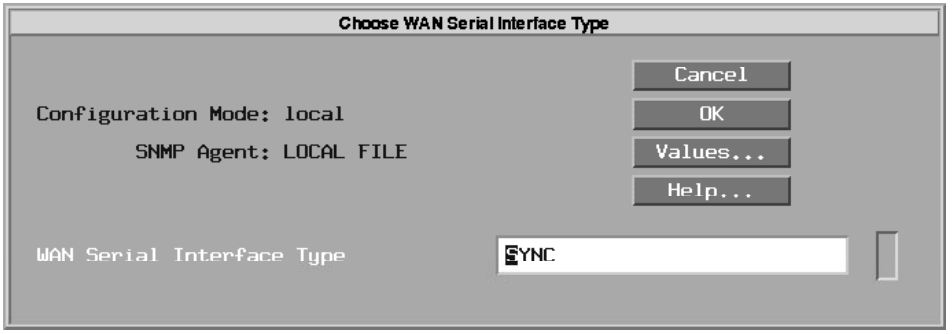

Figure 1-4. Choose WAN Serial Interface Type Window

On the Backbone Link Node (BLN®) and Backbone Concentrator Node (BCN®), the Choose WAN Serial Interface Type window appears only for ports on an Octal Sync Link Module. For all other modules, Site Manager displays the Sync Line Media Type window (Figure 1-5).

If you are using synchronous PPP for your dial connections, accept the default, Sync, for the WAN Serial Interface Type parameter. Site Manager displays the Sync Line Media Type window (Figure 1-5). If you plan to use Asynchronous PPP for your dial connections, select Async. Site Manager displays the Async Line Media Type window (Figure 1-6).

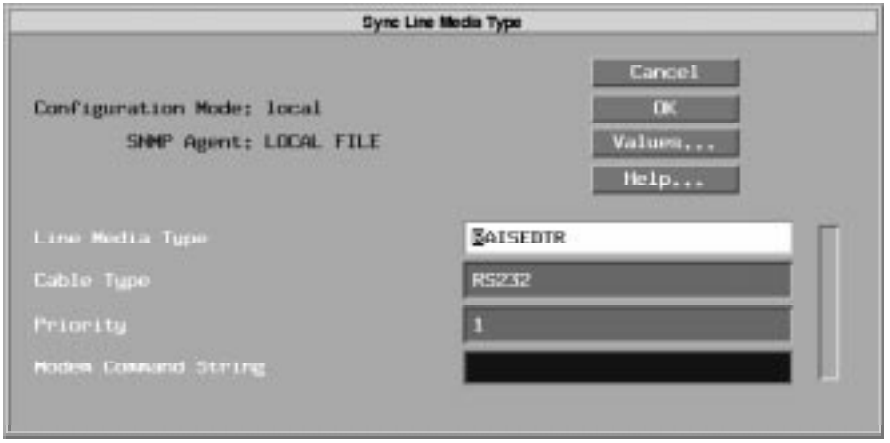

Figure 1-5. Sync Line Media Type Window

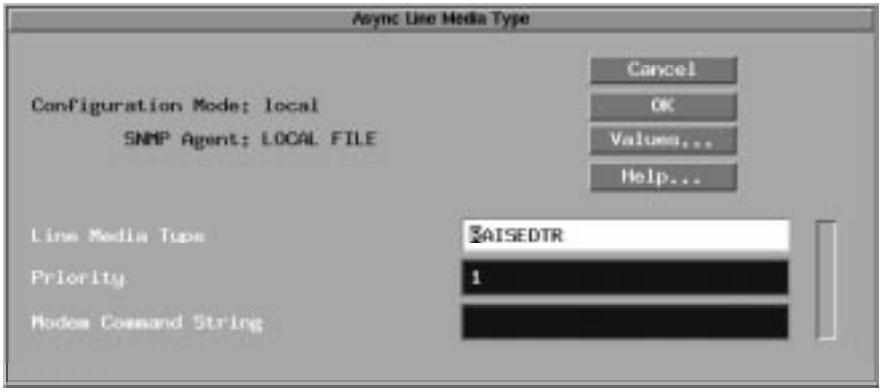

Figure 1-6. Async Line Media Type Window

Click on OK to accept the line media type defaults.

You return to the RADIUS Client Configuration window (refer to Figure 1-2). Go to Step 5.

- To configure an ISDN line for RADIUS, click on an ISDN, MCT1, or MCE1 connector.

  Site Manager displays the ISDN Switch Configuration window (Figure 1-7).

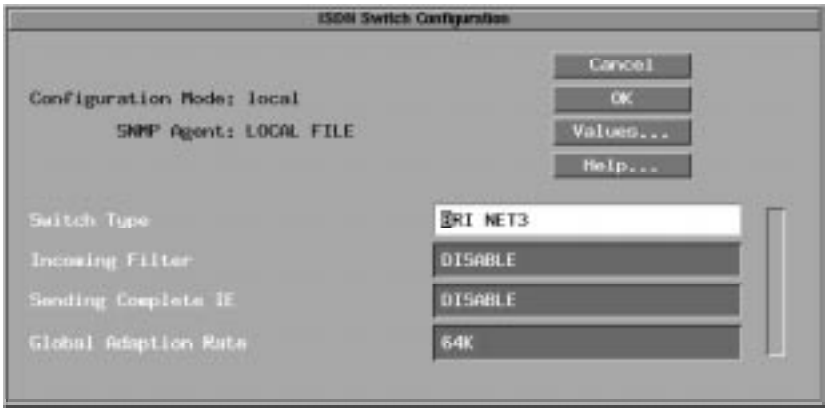

Figure 1-7. ISDN Switch Configuration Window

Click on OK to accept the defaults. Site Manager displays the ISDN Logical Lines window (Figure 1-8).

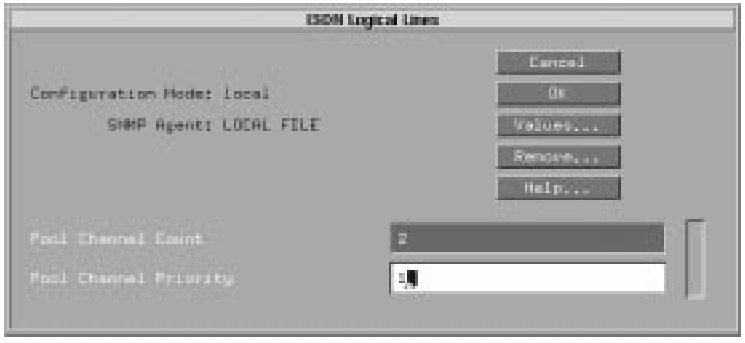

Figure 1-8. ISDN Logical Lines Window

Click on OK to accept the defaults.

You return to the RADIUS Client Configuration window (refer to Figure 1-2).

Site Manager adds the letters **DR** to the connector's name to designate it as a RADIUS interface.

5. **Keep the RADIUS Client Configuration window open and go to the next section, "Specifying the Client's IP Address."**

Specifying the Client's IP Address

To enable RADIUS, you must specify the client's Internet Protocol (IP) address. As the RADIUS client, the router passes this address to the server when a remote user makes an authentication or accounting request. The server does not accept the request without the client's IP address.

To configure the client's IP address:

1. **Enter an IP address for the Client IP Address parameter.**

Site Manager: Client IP Address parameter: page A-1

2. **Keep the RADIUS Client Configuration window open and go to the next section, "Specifying the Primary Server's IP Address."**

Specifying the Primary Server's IP Address

To enable RADIUS, you must specify the IP address of the RADIUS server. The first server you configure is the *primary server*. You can have only one primary server for each client.

To configure the primary server's IP address:

1. **Click on Server.**

   Site Manager displays the Primary Server Address window (Figure 1-9).

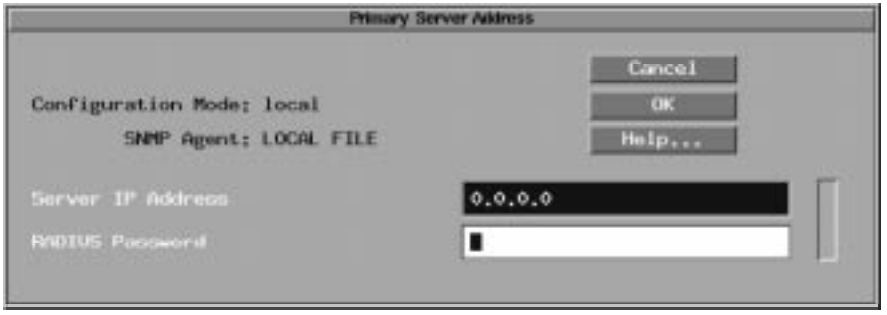

Figure 1-9. Primary Server Address Window

2. **Enter the IP address of the RADIUS server.**

Site Manager: Server IP Address parameter: page A-2

3. **Enter a password for the server.**

Site Manager: RADIUS Password parameter: page A-2

   The client and server must use the same password.

4. **Click on OK.**

   Site Manager displays the RADIUS Server Configuration window, which shows the parameter defaults for the server (Figure 1-10).

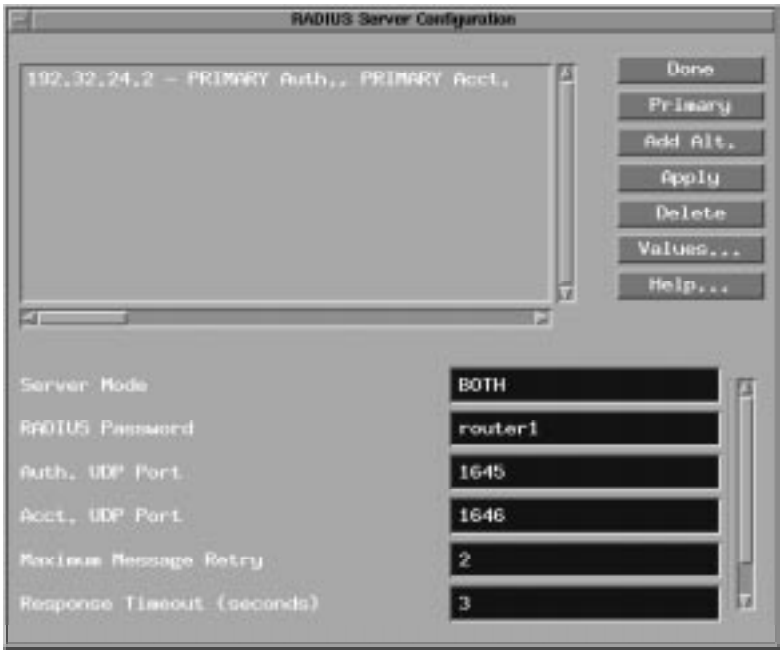

Figure 1-10. RADIUS Server Configuration Window

5. **Click on Done to accept the parameter defaults.**

   You return to the RADIUS Client Configuration window (refer to Figure 1-2).

6. **Keep the RADIUS Client Configuration window open and go to the next section, "Selecting a Protocol for RADIUS Authentication."**

Selecting a Protocol for RADIUS Authentication

For RADIUS authentication, you must select a protocol. Once you select a protocol, the RADIUS client automatically configures an unnumbered circuit interface for the protocol. An unnumbered circuit interface has an address of 0.0.0.0, which means that the circuit is not restricted to a specific remote destination address. This enables the client to use the circuit for many remote users.

To select a protocol for RADIUS authentication:

1. **Click on Dial-In Protocol.**

   Site Manager displays the RADIUS Dial_In Slot window (Figure 1-11).

Figure 1-11. RADIUS Dial_In Slot Window

2. **Enter the number of a slot configured for authentication, then click on OK.**

Site Manager: Slot Number parameter: page A-5

   Site Manager displays the RADIUS Dial_In Protocol window (Figure 1-12).

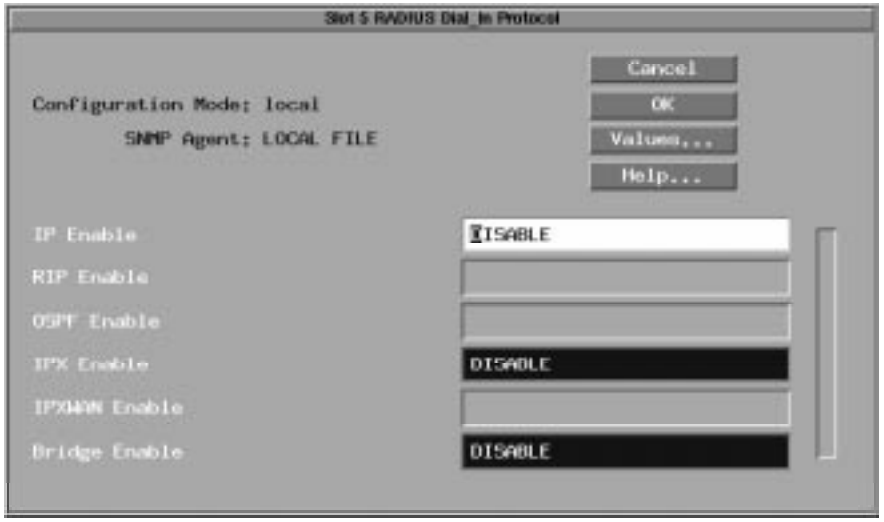

Figure 1-12. RADIUS Dial_In Protocol Window

3. **Select Enable for the protocol you want to use, then click on OK.**

   Refer to Appendix A for parameter descriptions of each protocol.

   If your network uses only dial-up lines, we recommend that you enable IP together with RIP or the Internet Packet Exchange (IPX) protocol. When you enable these parameters, Site Manager displays a window that asks if the remote site is using dial optimized routing (Figure 1-13).

Figure 1-13. Dial Optimized Routing Query Window

If the remote site is using dial optimized routing, click on OK. Site Manager automatically modifies several routing update parameters so the client can operate with dial optimized routing.

If your network uses a combination of leased lines and dial-up lines (for example, using dial backup service to support leased connections), it is unlikely that the routers use dial optimized routing, so click on Cancel. Site Manager will not modify the routing update parameters.

After you respond to the window, you return to the RADIUS Dial_In Protocol window.

4. **Click on OK.**

   You return to the RADIUS Client Configuration window (refer to Figure 1-2).

5. **Click on Done to return to the Configuration Manager window.**

Chapter 2
RADIUS Overview

Remote access is a rapidly growing segment of the networking industry. Users in branch offices, sales people in the field, and telecommuters are just a few of the people who rely on remote access to do their jobs. Internet service providers (ISPs) want to offer more remote-access services to their customers and control the billing of those services. As networks grow to accommodate more users, network security and billing become more difficult to manage.

RADIUS solves these issues by centralizing security and accounting information. This improves security and provides a solution that can adapt to the changing size and needs of remote users and service providers.

How RADIUS Works

A RADIUS application has two components, the RADIUS *server* and the RADIUS *client*.

The RADIUS server is a computer equipped with server software (for example, a UNIX workstation) that is located at a central office or campus. It has authentication and access information in a form that is compatible with the client. A network can have one server for both authentication and accounting, or one server for each service.

The RADIUS client can be a router or a remote-access server that is equipped with client software and typically resides on the same local area network (LAN) segment as the server. The client is the network access point between the remote users and the server.

RADIUS authentication lets you identify remote users before you give them access to a central network site. *RADIUS accounting* enables the server to collect data during a remote user's dial-in session with the client. The server can then determine billing charges.

Figure 2-1 shows a sample network using RADIUS.

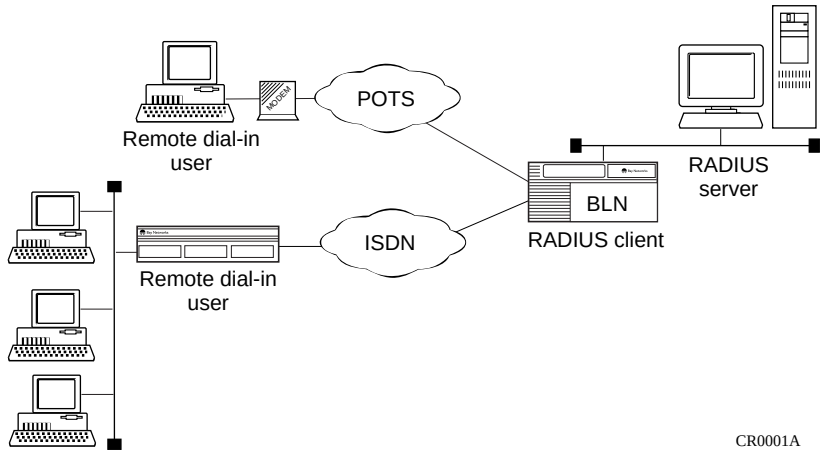

Figure 2-1. Sample Network Using RADIUS

Bay Networks RADIUS Implementation

The following Bay Networks platforms can operate as RADIUS clients:

- Backbone Link Node (BLN)
- Backbone Concentrator Node (BCN)
- Access Stack Node (ASN™)

As a RADIUS client, the router can support accounting, authentication, or both. The number of remote users that the client can support at one time is equal to the number of active dial-up connections.

The client can also support a *primary server*, which is the original destination server, and an *alternate server*, which is a server that the client contacts if it cannot reach the primary server.

RADIUS Authentication

You configure RADIUS authentication on a slot-by-slot basis. Therefore, a call designated for a RADIUS-configured slot performs authentication. If the router is already using a slot for dial-on-demand, dial backup, or bandwidth-on-demand service, you cannot configure this slot for authentication.

When a remote user calls the RADIUS client, the client passes the call request, referred to as the *access challenge*, to the RADIUS server. The access challenge contains the user's name and password. The server verifies the user's identity and, for authorized callers, responds with an *access accept* message, which includes the required access information. This information is sent to the client, which passes it to the remote user. If the remote user is not authorized, the server responds with an *access reject* message.

The client can pass multiple requests to the server simultaneously. If the client cannot reach the server, and you configured an alternate server, the client passes the request to the alternate server.

The authentication process occurs only once for each call. Once RADIUS authentication is complete, the remote user can communicate with the destination network.

Using PPP for Dial-up Connections

The Bay Networks RADIUS client uses Point-to-Point Protocol (PPP) for the dial-up line between itself and the remote user. When you configure RADIUS, Site Manager automatically configures PPP for the client.

To identify itself to the server, the remote user uses the PPP Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP). The client includes the remote user's CHAP name and secret or PAP ID and password in the access challenge to the server.

Using IP and IPX Unnumbered Protocols for PPP Connections

The RADIUS client supports only IP and IPX unnumbered interfaces, which means that the circuit's interface address is 0.0.0.0. All remote users that dial in to the same slot on the client receive the same unnumbered protocol configuration.

Note: Unlike the circuit's address, the RADIUS client's address is a numbered address.

The unnumbered circuit interface eliminates the need for a unique circuit configuration for each remote user in a network. Therefore, an unnumbered circuit interface reduces the configuration effort and the number of IP addresses that you use for a large network. The client can activate any available circuit for an incoming call because there is no specific address assigned to the circuit.

When you configure authentication for a router slot, Site Manager automatically configures the dial-up circuits required for the client to accept calls from the remote user. You are responsible for configuring only the unnumbered circuit interfaces.

In addition to configuring unnumbered circuit interfaces, we recommend that you enable IP or IPX triggered updates for the RADIUS client. The client uses triggered updates to provide its local area network (LAN) with routing information from the remote router. Refer to *Configuring IP Services* or *Configuring IPX Services* for more information about triggered updates.

Configuring the Remote User to Work with the RADIUS Client

In most RADIUS networks, the remote user is a router. To enable the remote router to work with the RADIUS authentication client, follow these guidelines:

- Enable dial optimized routing.

  The remote router sends routing updates to advertise its LAN to the client. By enabling dial optimized routing, you reduce the frequency of routing updates, which prevents the line from remaining active unnecessarily.

- Configure one-way PPP authentication.

  The remote router must support one-way PPP authentication, which means that only the client sends CHAP challenges or PAP authentication requests to the remote user. The remote user only recognizes and responds to the CHAP challenges or PAP authentication requests from the client.

- Configure a default route in the routing table of the remote router.

  The client does not advertise its LAN to the remote router. To specify the path from the remote router to the client, you configure a default route, which is a static route that enables the remote router to contact the client.

Refer to Appendix C for configuration examples.

RADIUS Accounting

You configure RADIUS accounting on a slot-by-slot basis. Therefore, a call designated for a RADIUS-configured slot performs RADIUS accounting.

The RADIUS accounting server calculates billing charges for a communication session between the remote user and the client. The RADIUS client sends information to the server, such as the status of each call and the number of packets transmitted during the session. Using this data, the server determines billing charges, which the network administrator can use to manage network costs.

An *accounting session* is the time during which the remote user communicates with the client. The session begins when the client passes an accounting request from the remote user to the server, with an accounting status byte set to **start**. The session ends when the client sends a second request with the accounting status byte set to **stop**. Multiple accounting sessions can occur simultaneously if there are multiple dial-up connections.

The client sends accounting requests only to the server configured for accounting, which enables you to use different servers for accounting and authentication.

If the client cannot reach the primary server after several attempts, and you configured an alternate server, the client sends the accounting request to the alternate server. If an accounting session starts with the primary server, and this server goes down, the session is continued with the alternate server. Unless the primary server recovers, the request to end the session is then sent to the alternate server. To accurately determine billing charges, the network administrator collects information from all accounting servers.

Using PPP for Dial-up Connections

The Bay Networks client uses PPP for the dial-up line between itself and the remote user. When you configure RADIUS, Site Manager automatically configures PPP for the client.

Configuring a Dial Service for RADIUS Accounting

To use RADIUS accounting on the router, you must configure at least one of the three Bay Networks dial services: dial-on-demand, dial backup, or bandwidth-on-demand. The dial service enables the router to activate a dial-up connection when it receives an incoming call. For information about dial services, refer to *Configuring Dial Services*.

Using RADIUS-Compatible Servers with the RADIUS Client

The Bay Networks RADIUS client can communicate with any RADIUS-compatible server. You must configure the server's IP address so that the client can communicate with the server.

To ensure that a server is always available, you can configure one primary server and multiple alternate servers. The client tries to connect to the primary server first. If the primary server does not respond after a certain number of attempts, the client sends the authentication or accounting request to the alternate server. Once the primary server recovers, the client resumes communication with the primary server.

Accepting Remote Users' IP Addresses

The client accepts the IP address of a remote user only if the remote user is a PC, not another router. The client does not support any other RADIUS extensions.

For More Information

Refer to the following sources for more information about RADIUS:

Aboba, B., Zorn, G. “RADIUS Client MIB.” Internet Draft. March 1997.

Aboba, B., Zorn, G. “RADIUS Server MIB.” Internet Draft. March 1997.

Aboba, B., Zorn, G. “Implementation of Mandatory Tunneling via RADIUS.” Internet Draft. March 1997.

Internet Engineering Task Force World Wide Web site: http://ftp.ietf.org/.

Rigney, C. “RADIUS Accounting.” RFC 2139. April 1997.

Rigney, C., Rubens A., Simpson, W.A., Willens, S. “Remote Authentication Dial In User Service (RADIUS).” RFC 2138. April 1997.

Rigney, C., Willats, W. “RADIUS Extensions.” Internet Draft. January 1997.

Zorn, G. “RADIUS Attributes for Tunnel Protocol Support.” Internet Draft. March 1997.

Zorn, G. “Extensible RADIUS Attributes for Tunnel Protocol Support.” Internet Draft. March 1997

Chapter 3
Customizing the RADIUS Client Configuration

This chapter describes the changes you can make to the RADIUS client's configuration.

Modifying the Client's IP Address

You should have already configured an IP address for the client in Chapter 1.

To modify the address of the client, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit RADIUS.**

   Site Manager displays the RADIUS Client Configuration window (Figure 3-1).

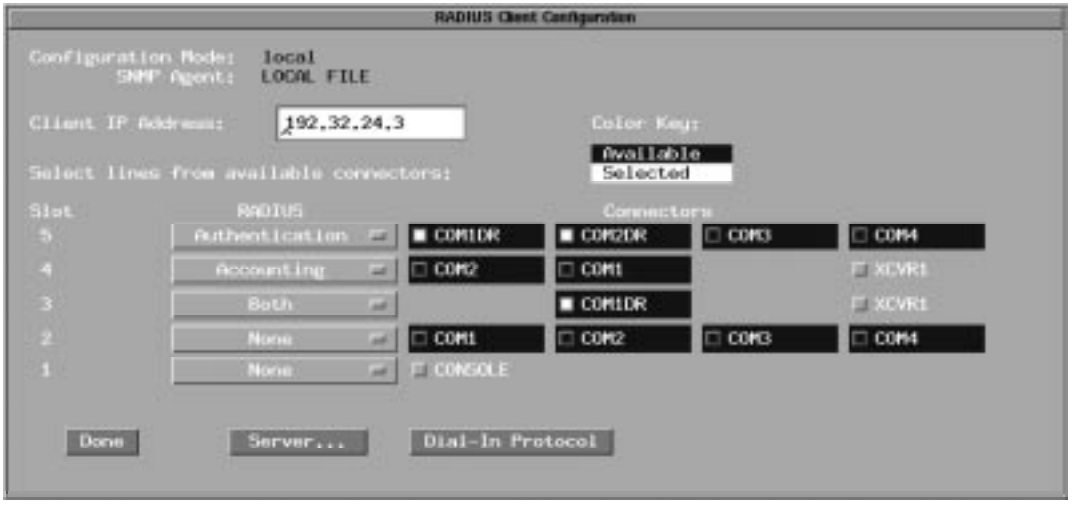

Figure 3-1. RADIUS Client Configuration Window

2. **Enter a new IP address for the Client IP Address parameter.**

Site Manager: Client IP Address parameter: page A-1

3. **Click on Done to return to the Configuration Manager window.**

Modifying Service from Authentication to Accounting

You can change the service from RADIUS authentication to accounting without having to remove authentication. You may also want to use both services. To change from accounting to authentication, you must remove accounting service from the slot and then configure authentication service.

To modify service, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit RADIUS.**

   Site Manager displays the RADIUS Client Configuration window (refer to Figure 3-1). This window shows the slots and their current configuration.

2. **Click on the box labeled Authentication, then select Accounting or Both.**

   The service you select is now operating for that slot.

3. **If necessary, modify the client and server addresses and protocol configurations to accommodate the new service.**

4. **Click on Done to return to the Configuration Manager window.**

Modifying the Protocol for RADIUS Authentication

To modify the unnumbered protocol for RADIUS authentication, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit RADIUS.**

   Site Manager displays the RADIUS Client Configuration window (refer to Figure 3-1).

2. **Click on Dial-In Protocol.**

   Site Manager displays the RADIUS Dial_In Slot window (Figure 3-2).

Figure 3-2. RADIUS Dial_In Slot Window

3. **Enter the number of a slot configured for RADIUS, then click on OK.**

Site Manager: Slot Number parameter: page A-5

   Site Manager displays the RADIUS Dial_In Protocol window (Figure 3-3).

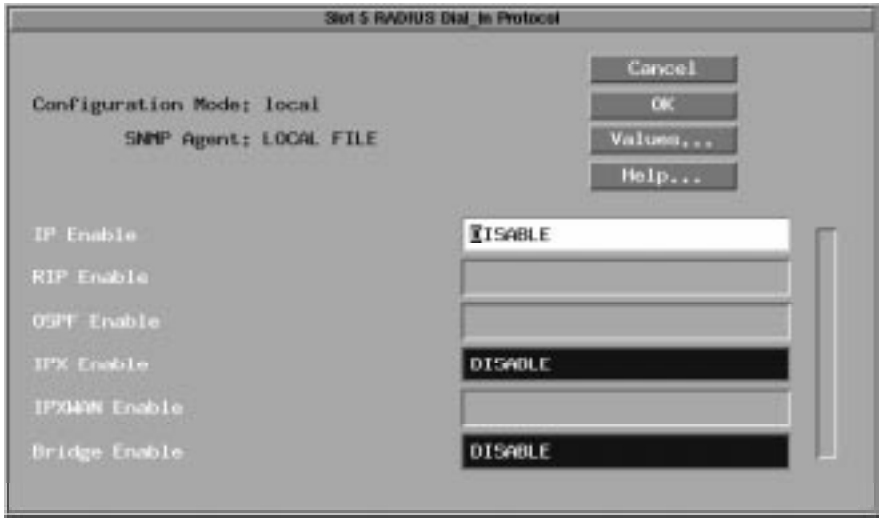

Figure 3-3. RADIUS Dial_In Protocol Window

4. **Set the enabled protocol to Disable, and set the protocol you want to use to Enable.**

   Refer to Appendix A for parameter descriptions of each protocol.

   If your network uses only dial-up lines, we recommend that you enable IP together with RIP or IPX. When you enable these parameters, Site Manager displays a window that asks if the remote site is using dial optimized routing (Figure 3-4).

Figure 3-4. Dial Optimized Routing Query Window

If the remote site is using dial optimized routing, click on OK. Site Manager automatically modifies several routing update parameters so the client can operate with dial optimized routing.

If your network uses a combination of leased lines and dial-up lines (for example, using dial backup service to support leased connections), it is unlikely that the routers use dial optimized routing, so click on Cancel. Site Manager will not modify the routing update parameters.

After you respond to the window, you return to the RADIUS Dial_In Protocol window.

5. **Click on OK.**

   You return to the RADIUS Client Configuration window (refer to Figure 3-1).

6. **Click on Done to return to the Configuration Manager window.**

Modifying the PPP Authentication Protocol

The remote user identifies itself to the server using one of the PPP authentication protocols, CHAP or PAP. It includes either a CHAP name and secret or a PAP ID and password in the access challenge to the server. CHAP is the default authentication protocol. For more information about PPP, refer to *Configuring PPP Services*.

To change the authentication protocol to PAP, begin at the Configuration Manager window:

1. **Select Protocols > PPP > Interfaces.**

   Site Manager displays the PPP Interface List window (Figure 3-5).

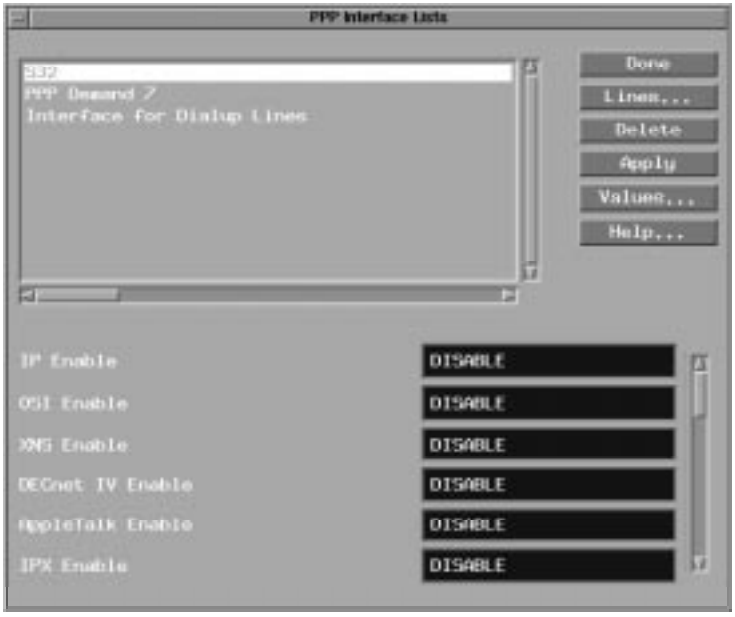

Figure 3-5. PPP Interface List Window

2. **Select the Interface for Dialup Lines record, then click on Lines.**

   Site Manager displays the PPP Line Lists window (Figure 3-6).

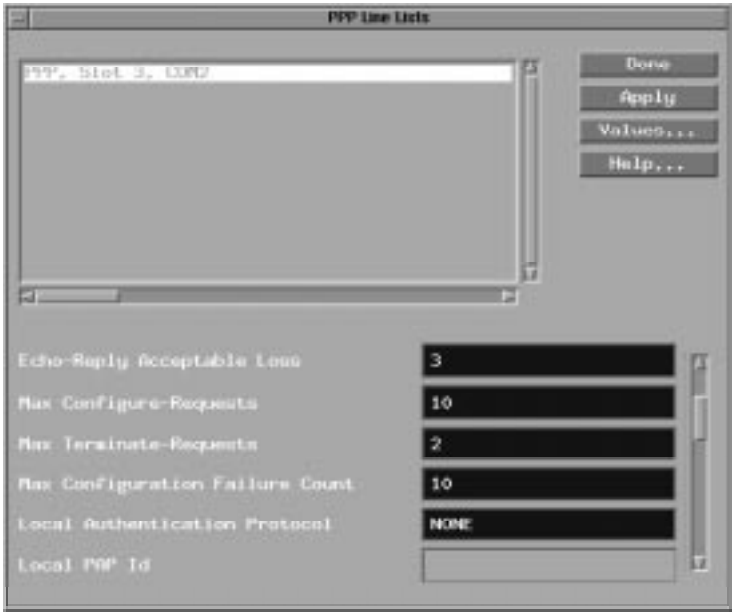

Figure 3-6. PPP Line Lists Window

3. **Select PAPAUTH as the value for the Local Authentication Protocol parameter.**
4. **Click on Done.**

   You return to the PPP Interface List window (refer to Figure 3-5).
5. **Click on Done to return to the Configuration Manager window.**

Removing RADIUS Authentication and Accounting

To remove RADIUS authentication and accounting from a slot, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit RADIUS.**

   Site Manager displays the RADIUS Client Configuration window (refer to Figure 3-1).

2. **Click on the box labeled Authentication, Accounting, or Both, then select None.**

   Site Manager removes RADIUS from that slot.

3. **Click on Done to return to the Configuration Manager window.**

Chapter 4
Customizing the RADIUS Server Configuration

This chapter explains how to modify the RADIUS server configuration. The server parameters tell the client how the server is configured and define how the client and server communicate.

Modifying the Primary Server's Password

The first server you configure is the *primary server*. You can have only one primary server for each client. You should have already entered the server's IP address in Chapter 1.

To modify the primary server's password, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit Server.**

   Site Manager displays the RADIUS Server Configuration window, which shows the parameter defaults for the server configuration (Figure 4-1).

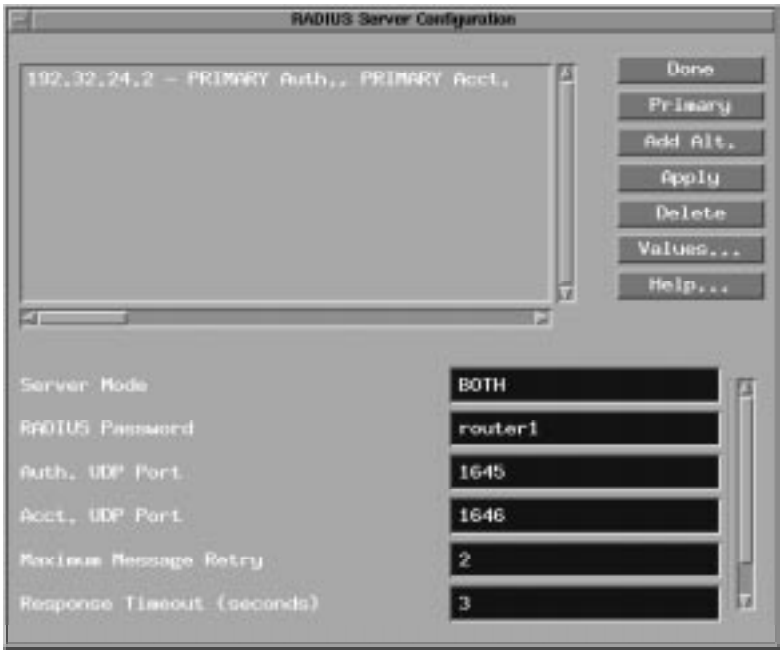

Figure 4-1. RADIUS Server Configuration Window

2. **Enter a new password, then click on Apply.**

Site Manager: RADIUS Password parameter: page A-2

3. **Click on Done to return to the Configuration Manager window.**

Modifying the Server Mode

The server mode tells the client how the server is configured. You may want to change the service from RADIUS authentication to accounting or from accounting to authentication. You may also want to use both services.

To modify the server mode, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit Server.**

   Site Manager displays the RADIUS Server Configuration window (refer to Figure 4-2).

2. **Enter a value for the Server Mode parameter, then click on Apply.**

Site Manager: Server Mode parameter: page A-2

3. **Click on Done to return to the Configuration Manager window.**

Authentication and Accounting UDP Ports

The User Datagram Protocol (UDP) port is the logical port that designates data for the RADIUS application on the server. The UDP port is typically included in an IP datagram.

The default values for the authentication and accounting UDP ports follow the RADIUS RFC specifications. In general, you should not change these values.

Refer to Appendix A for parameter descriptions.

Modifying the Server Response Time

When the client sends an accounting or authentication request to the server, you can specify how long the client waits for a response from the server. If the client does not receive a response, it retransmits the request. This waiting period prevents network operations from slowing down.

To modify the server response time, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit Server.**

   Site Manager displays the RADIUS Server Configuration window (refer to Figure 4-2).

2. **Enter a value for the Response Timeout parameter, then click on Apply.**

Site Manager: Response Timeout (seconds) parameter: page A-4

3. **Click on Done to return to the Configuration Manager window.**

Modifying the Number of Client Requests to the Server

You can modify the number of times the client sends a request to the server before the client considers the server unreachable. If the server is located at a distance from the client, you may want to set the number of requests to a higher value than the default.

To modify the number of client requests to the server, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit Server.**

   Site Manager displays the RADIUS Server Configuration window (refer to Figure 4-2).

2. **Enter a new value for the Maximum Message Retry parameter, then click on Apply.**

Site Manager: Maximum Message Retry parameter: page A-3

3. **Click on Done to return to the Configuration Manager window.**

Configuring Alternate Servers

In addition to the primary server, you can configure one or more alternate RADIUS servers. An alternate server ensures that you can maintain network security and accounting in case the primary server fails. You must configure a primary server before you configure an alternate server. After that, you can configure multiple alternate servers for each client.

To configure an alternate server, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit Server.**

   Site Manager displays the RADIUS Server Configuration window (Figure 4-2).

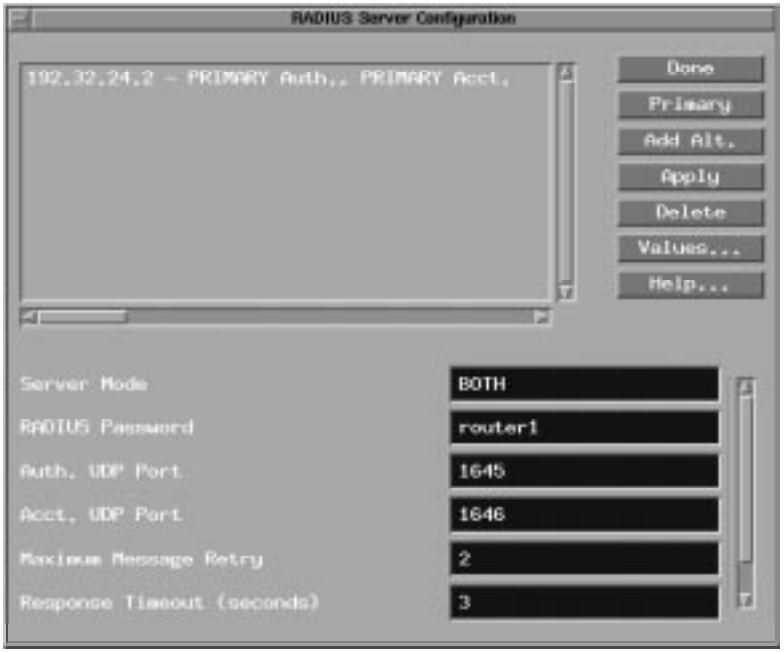

Figure 4-2. RADIUS Server Configuration Window

2. **Click on Add Alt.**

   Site Manager displays the Alternate Server Address window (Figure 4-3).

Figure 4-3. Alternate Server Address Window

3. **Enter the IP address of the alternate RADIUS server.**

Site Manager: Server IP Address parameter: page A-2

4. **Enter a password for the RADIUS server.**

Site Manager: RADIUS Password parameter: page A-2

5. **Click on OK.**

   You return to the RADIUS Server Configuration window (refer to Figure 4-2), which lists the alternate server.

6. **Click on Done to return to the Configuration Manager window.**

Reconnecting to the Primary Server

If the primary server fails, you can instruct the client to use an alternate server, but after a specified time period, try to reconnect to the primary server.

To reconnect to the primary server, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit Server.**

   Site Manager displays the RADIUS Server Configuration window (refer to Figure 4-2).

2. **Enter a new value for the Server Reset Timer parameter, then click on Apply.**

Site Manager: Server Reset Timer (minutes) parameter: page A-4

3. **Click on Done to return to the Configuration Manager window.**

Changing the Primary and Alternate Servers

You can change which server is the primary and which is the alternate. Begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit Server.**

   Site Manager displays the RADIUS Server Configuration window (refer to Figure 4-2).

2. **Select an alternate server entry from the list.**
3. **Set the Server Mode parameter to the appropriate service.**

Site Manager: Server Mode parameter: page A-2

4. **Click on Primary.**

   Site Manager changes the entry in the list. The alternate server is now the primary server, and the original primary server is now the alternate server.

5. **Click on Done to return to the Configuration Manager window.**

Removing a Server Entry

To remove a server entry from the RADIUS configuration, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Edit Server.**

   Site Manager displays the RADIUS Server Configuration window (refer to Figure 4-2).

2. **Select a server entry, then click on Delete.**

   Site Manager removes the entry from the list.

3. **Click on Done to return to the Configuration Manager window.**

Appendix A
RADIUS Parameters

This appendix describes each of the RADIUS parameters. Each description includes the path of Site Manager windows that you follow to find the parameter. Each path assumes that you begin at the Configuration Manager window.

You can use Site Manager to modify all RADIUS parameters. You can also use the Technician Interface to modify parameters by issuing **set** and **commit** commands with the Management Information Base (MIB) object ID. This process is the same as modifying parameters using Site Manager. For information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Client IP Address Parameter

Parameter:	**Client IP Address**
Path:	Protocols > Global Protocols > RADIUS > Create RADIUS or Protocols > Global Protocols > RADIUS > Edit RADIUS
Default:	None
Options:	A 32-bit IP address
Function:	Identifies the RADIUS client.
Instructions:	Enter an IP address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.22.1.1.5

Server Configuration Parameters

Parameter: **Server IP Address**

Path: Protocols > Global Protocols > RADIUS > Create RADIUS > **Server**
or
Protocols > Global Protocols > RADIUS > Edit Server

Default: None

Options: A 32-bit IP address

Function: Identifies the RADIUS server.

Instructions: Enter an IP address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.2.1.3

Parameter: **Server Mode**

Path: Protocols > Global Protocols > RADIUS > Edit Server

Default: Both

Options: Authentication | Accounting | Both

Function: Specifies the RADIUS operation for this port.

Instructions: Select the service you want for this port. If you want to configure both authentication and accounting, select Both.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.2.1.4

Parameter: **RADIUS Password**

Path: Protocols > Global Protocols > RADIUS > Edit Server

Default: None

Options: An alphanumeric string, up to a maximum of 64 characters

Function: Identifies the client to the server. The client and server must use the same password.

Instructions: Enter a password that contains a maximum of 64 characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.2.1.11

Parameter: Auth. UDP Port

Path: Protocols > Global Protocols > RADIUS > Edit Server
Default: 1645
Options: An integer specifying the UDP logical port for authentication
Function: Designates a data packet for RADIUS authentication. This number is required for access to the authentication server.
Instructions: Accept the default.
MIB Object ID: 1.3.6.1.4.1.18.3.5.22.2.1.6

Parameter: Acct. UDP Port

Path: Protocols > Global Protocols > RADIUS > Edit Server
Default: 1646
Options: An integer specifying the UDP logical port for accounting
Function: Designates a data packet for RADIUS accounting. This number is required for access to the accounting server.
Instructions: Accept the default.
MIB Object ID: 1.3.6.1.4.1.18.3.5.22.2.1.9

Parameter: Maximum Message Retry

Path: Protocols > Global Protocols > RADIUS > Edit Server
Default: 2
Options: 1 to 10
Function: Specifies the number of times the RADIUS client retransmits a request before it considers the RADIUS server unreachable.
Instructions: Enter the number of times you want the client to retransmit a request.
MIB Object ID: 1.3.6.1.4.1.18.3.5.22.2.1.13

Parameter:	**Response Timeout (seconds)**
Path:	Protocols > Global Protocols > RADIUS > Edit Server
Default:	3
Options:	1 to 60
Function:	Specifies the number of seconds the RADIUS client waits before retransmitting a request to the RADIUS server.
Instructions:	Accept the default or enter a number of seconds in the range 1 to 60.
MIB Object ID:	1.3.6.1.4.1.18.3.5.22.2.1.12

Parameter:	**Server Reset Timer (minutes)**
Path:	Protocols > Global Protocols > RADIUS > Edit Server
Default:	10
Options:	1 to 60
Function:	Specifies the number of minutes the RADIUS client waits before retrying the primary server after it fails to respond. If the primary server fails to respond, the client considers it unreachable and switches to the alternate server. After this specified time period, the client tries to reconnect to the primary server.
Instructions:	Accept the default or enter the number of minutes you want the client to wait for the primary server to recover.
MIB Object ID:	1.3.6.1.4.1.18.3.5.22.2.1.14

Protocol Parameters for RADIUS Authentication

These protocols are only for RADIUS authentication.

Parameter: Slot Number

Path: Protocols > Global Protocols > RADIUS > Edit RADIUS > Dial-In Protocol > RADIUS Dial_In Slot
Default: None
Options: An integer that represents a router slot configured for RADIUS
Function: Identifies the slot configured for RADIUS.
Instructions: Enter the slot number.
MIB Object ID: 1.3.6.1.4.1.18.3.5.22.2.1.4

Parameter: IP Enable

Path: Protocols > Global Protocols > RADIUS > Edit RADIUS > Dial-In Protocol > RADIUS Dial_In Slot > RADIUS Dial_In Protocol
Default: Disable
Options: Enable | Disable
Function: Enables or disables IP on this interface.
Instructions: Select Enable to enable IP on this interface.
MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.12.1.5

Parameter: RIP Enable

Path: Protocols > Global Protocols > RADIUS > Edit RADIUS > Dial-In Protocol > RADIUS Dial_In Slot > RADIUS Dial_In Protocol
Default: Disable
Options: Enable | Disable
Function: Enables or disables RIP on this interface.
Instructions: Select Enable to enable RIP on this interface.
MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.12.1.7

Parameter: OSPF Enable

Path: Protocols > Global Protocols > RADIUS > Edit RADIUS > Dial-In Protocol > RADIUS Dial_In Slot > RADIUS Dial_In Protocol

Default: Disable

Options: Enable │ Disable

Function: Enables or disables OSPF on this interface.

Instructions: Select Enable to enable OSPF on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.12.1.8

Parameter: IPX Enable

Path: Protocols > Global Protocols > RADIUS > Edit RADIUS > Dial-In Protocol > RADIUS Dial_In Slot > RADIUS Dial_In Protocol

Default: Disable

Options: Enable │ Disable

Function: Enables or disables IPX on this interface.

Instructions: Select Enable to enable IPX on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.12.1.9

Parameter: IPXWAN Enable

Path: Protocols > Global Protocols > RADIUS > Edit RADIUS > Dial-In Protocol > RADIUS Dial_In Slot > RADIUS Dial_In Protocol

Default: Disable

Options: Enable │ Disable

Function: Enables or disables IPXWAN on this interface.

Instructions: Select Enable to enable IPXWAN on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.12.1.13

Parameter: Bridge Enable

Path: Protocols > Global Protocols > RADIUS > Edit RADIUS > Dial-In Protocol > RADIUS Dial_In Slot > RADIUS Dial_In Protocol

Default: Disable

Options: Enable │ Disable

Function: Enables or disables bridging on this interface.

Instructions: Select Enable to enable bridging on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.12.1.10

Appendix B
RADIUS Parameter Defaults

Table B-1 lists the default settings for the RADIUS parameters.

Table B-1. RADIUS Parameter Defaults

Parameter	Default
Client IP Address	None
Server IP Address	None
RADIUS Password	None
Server Mode	Both
Auth. UDP Port	1645
Acct. UDP Port	1646
Maximum Message Retry	2
Response Timeout (seconds)	3
Server Reset Timer (minutes)	10
Slot Number	None
IP Enable	Disable
RIP Enable	Disable
OSPF Enable	Disable
IPX Enable	Disable
IPXWAN Enable	Disable
Bridge Enable	Disable

Appendix C
Configuration Examples

This appendix provides the following configuration examples for a router acting as a RADIUS client:

- Configuring RADIUS authentication
- Configuring RADIUS accounting
- Configuring RADIUS authentication and accounting

The examples show only those parameters whose defaults you must change for proper configuration. The examples do not show any configuration windows. For dial service windows, refer to *Configuring Dial Services*; for RADIUS windows, refer to the appropriate chapter in this manual.

Configuring RADIUS Authentication

This example explains how to configure the router as a RADIUS authentication client, and assumes the following:

- The client is a BLN.
- The network connections are all Raise DTR modem connections.
- The WAN serial interface type is synchronous.
- IP and RIP are the protocols for the client's unnumbered circuit interface.
- Dial optimized routing and one-way authentication are configured on the remote routers.
- A default route of 0.0.0.0 is configured on the remote routers to contact the client.

Figure C-1 shows the sample network for this example.

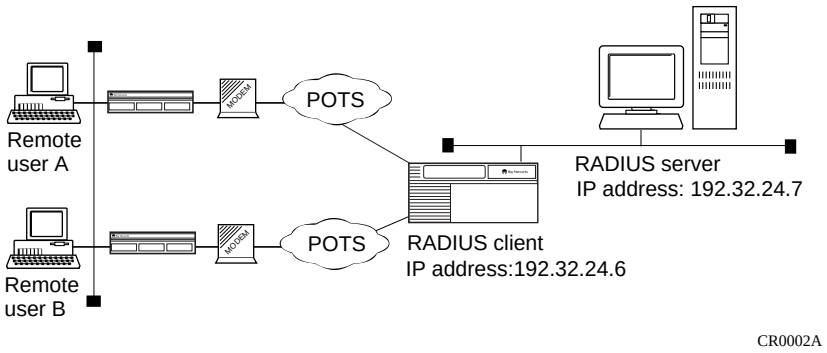

Figure C-1. Sample Network Using RADIUS Authentication

Before You Begin

Before you begin, do the following:

1. Create and save a configuration file with at least one PPP interface.
2. Retrieve the configuration file in local, remote, or dynamic mode.
3. Specify the router hardware if this is a local-mode configuration.

Enable RADIUS Authentication

To enable RADIUS authentication, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Create RADIUS.**

   Site Manager displays the RADIUS Client Configuration window, which lists the slots available for configuring RADIUS.

2. **To configure a slot for RADIUS, click on the box labeled None.**

   Site Manager displays a menu showing the RADIUS options.

3. **Select Authentication for the slot.**

4. **Click on the slot's COM connectors that you want to enable for RADIUS.**

   These connectors are automatically enabled for RADIUS operation.

   Once a connector is enabled for RADIUS, Site Manager adds the letters **DR** to the connector's name to designate it as a RADIUS interface.

5. **Enter 192.32.24.6 for the Client IP Address parameter.**

6. **Click on Server at the bottom of the window.**

   Site Manager displays the Primary Server Address window.

7. **Enter 192.32.24.7 for the Server IP Address parameter.**

8. **Enter Client_BLN for the RADIUS Password parameter, then click on OK.**

   Site Manager displays the RADIUS Server Configuration window, which shows the default configuration for the server.

9. **Accept the defaults for the server configuration parameters.**

10. **Click on Done.**

    You return to the RADIUS Client Configuration window.

11. **Go to the next section, "Select IP."**

Select IP

From the RADIUS Client Configuration window:

1. **Click on Dial-In Protocol.**

   Site Manager displays the RADIUS Dial_In Slot window.

2. **Enter the number of the slot configured for RADIUS, then click on OK.**

   Site Manager displays the RADIUS Dial_In Protocol window.

3. **Select Enable for the IP Enable parameter.**

4. **Select Enable for the RIP Enable parameter.**

5. **Click on OK.**

   Site Manager displays a window that asks if the remote site is using dial optimized routing. The remote routers in this example are using dial optimized routing.

6. **Click on OK.**

   Site Manager modifies the values of several routing update parameters; however, these changes are transparent to you.

   You return to the RADIUS Client Configuration window.

7. **Click on Done to return to the Configuration Manager window.**

Configuring RADIUS Accounting

This example explains how to configure the router as a RADIUS accounting client, and assumes the following:

- The client is an ASN.
- Dial backup is the dial service.
- The RADIUS client only receives calls, it does not make calls; therefore, you do not need to configure an outgoing phone list and local CHAP name and secret for the client.
- The leased and dial backup connections are using PPP.
- The WAN serial interface type is synchronous.
- RADIUS authentication is not configured on the client.

Figure C-2 shows the sample network for this example.

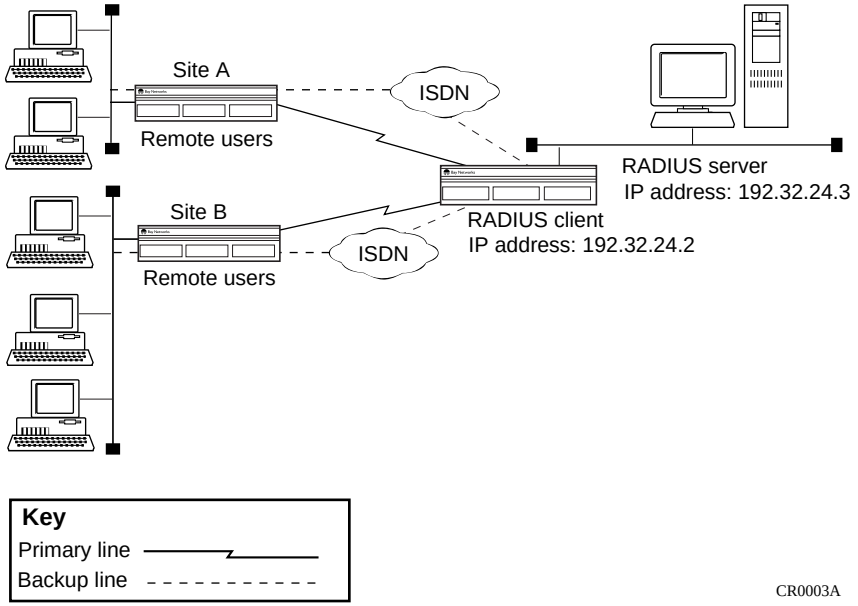

Figure C-2. Sample Network Using RADIUS Accounting

Before You Begin

Before you begin, do the following:

1. Create and save a configuration file with at least one PPP interface.
2. Retrieve the configuration file in local, remote, or dynamic mode.
3. Specify the router hardware if this is a local-mode configuration.

Create a Backup Pool

To create a backup pool, begin at the Configuration Manager window:

1. **Select an ISDN connector.**

   Site Manager displays the Port Application window.

2. **Click on OK to accept the default for the Port Application Mode parameter, Dialup 2B + D.**

   This configures the BRI interface. Repeat Steps 1 and 2 to configure additional BRI interfaces.

3. **Select Dialup > Backup Pools.**

   Site Manager displays the Backup Pools window.

4. **Click on Add.**

   Site Manager displays the Backup Pools Configuration window.

5. **Enter a pool ID, then click on OK.**

   Site Manager displays the Backup Lines Definition window.

6. **Click on an ISDN connector to assign a line to the pool, following these guidelines:**

   - Site Manager does not allow you to select any lines that you configured as leased lines.
   - Lines in a backup pool may reside across slots.

   Site Manager displays the ISDN Switch Configuration window.

7. **Click on Done to accept the parameter defaults.**

   Site Manager displays the ISDN Logical Lines window.

8. **Click on OK to accept the parameter defaults.**

You return to the Backup Lines Definition window. The letter B (backup) appears next to the ISDN port to indicate that it is a backup line.

9. **Select File > Exit to exit the Backup Lines Definition window.**

   You return to the Backup Pools window, which has three new buttons (Edit, Apply, and Delete) that allow you to edit the new pool.

10. **Repeat Steps 3 through 9 to select additional lines for the pool.**

11. **Click on Done to return to the Configuration Manager window.**

Create a Dial Backup Circuit

To create a PPP backup circuit, begin at the Configuration Manager window:

1. **Select Backup Circuits > PPP.**

   Site Manager displays the Primary Circuit Definition window, which lists the leased circuits that you have configured.

2. **Select a circuit entry and click on Cct Type.**

   Site Manager displays the Circuit Options window.

3. **Enter Primary for the Circuit Type parameter.**

4. **Enter the ID of the backup pool that this circuit should use.**

5. **Click on OK.**

   You return to the Primary Circuit Definition window, which shows the parameter defaults supplied by Site Manager.

6. **Repeat Steps 2 through 5 to specify additional primary circuits.**

7. **Scroll down the Primary Circuit Definition window to the Backup Mode parameter.**

8. **Select a value for the Backup Mode parameter. The default is Master.**

   If this router is the master router, the peer router's backup mode must be set to Slave. If you set the backup mode to Slave, Site Manager prompts you for caller resolution information so the slave router can verify the identity of a remote caller.

   Refer to *Configuring Dial Services* for more information about dial backup circuits.

Enable RADIUS Accounting

To enable RADIUS accounting, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Create RADIUS.**

   Site Manager displays the RADIUS Client Configuration window.

2. **To configure a slot for RADIUS, click on the box labeled None.**

   Site Manager displays a menu showing the RADIUS options.

3. **Select Accounting for the slot.**

4. **Enter 192.32.24.2 for the Client IP Address parameter.**

5. **Click on Server at the bottom of the window.**

   Site Manager displays the Primary Server Address window.

6. **Enter 192.32.24.3 for the Server IP Address parameter.**

7. **Enter Client_ASN for the RADIUS Password parameter, then click on OK.**

   Site Manager displays the RADIUS Server Configuration window, which shows the default configuration for the server.

8. **Accept the defaults for the server configuration parameters.**

9. **Click on Done.**

   You return to the RADIUS Client Configuration window.

10. **Click on Done to return to the Configuration Manager window.**

Configuring RADIUS Accounting and Authentication

This example explains how to configure the router as a RADIUS accounting and authentication client. The sample network shows a remote router dialing an alternate site when the original destination is not accessible. The example assumes the following:

- The client is an ASN.
- Dial backup is the dial service.
- The leased connections are using Frame Relay.
- The backup connections are using PPP.
- IP and RIP are the protocols for the client's unnumbered circuit interface.

Figure C-3 shows the sample network for this example.

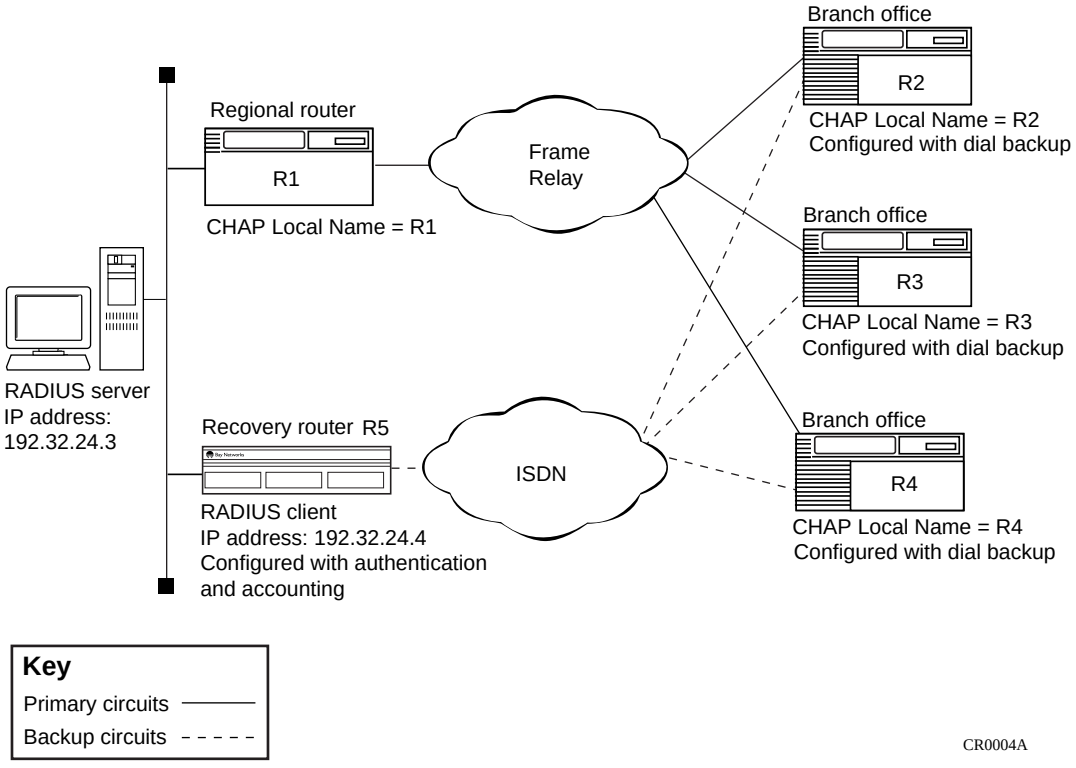

Figure C-3. Sample Network Configured for Dialing an Alternate Site

Before You Begin

Before you begin, do the following:

1. Create and save a configuration file with at least one Frame Relay interface.
2. Retrieve the configuration file in local, remote, or dynamic mode.
3. Specify the router hardware if this is a local-mode configuration.

Enable Dial Backup Service

To enable dial backup service, configure a dial backup pool and circuit according to the instructions in the previous section, "Configuring RADIUS Accounting. "

Enable RADIUS Accounting and Authentication

To enable RADIUS accounting and authentication, begin at the Configuration Manager window:

1. **Select Protocols > Global Protocols > RADIUS > Create RADIUS.**

   Site Manager displays the RADIUS Client Configuration window.

2. **To configure a slot for RADIUS, click on the box labeled None.**

   Site Manager displays a menu showing the RADIUS options.

3. **Select Both for the slot.**
4. **Click on the connectors that you want to configure as authentication interfaces.**
5. **Enter 192.32.24.4 for the Client IP Address parameter.**
6. **Click on Server at the bottom of the window.**

   Site Manager displays the Primary Server Address window.

7. **Enter 192.32.24.3 for the Server IP Address parameter.**
8. **Enter Client_ASN for the RADIUS Password parameter, then click on OK.**

   Site Manager displays the RADIUS Server Configuration window, which shows the default configuration for the server.

9. **Accept the defaults for the server configuration parameters.**

10. **Click on Done.**

    You return to the RADIUS Client Configuration window.

11. **Keep this window open and go to the next section, "Select IP for RADIUS Authentication."**

Select IP for RADIUS Authentication

From the RADIUS Client Configuration window:

1. **Click on Dial-In Protocol.**

   Site Manager displays the RADIUS Dial_In Slot window.

2. **Enter the number of the slot configured for RADIUS, then click on OK.**

   Site Manager displays the RADIUS Dial_In Protocol window.

3. **Select Enable for the IP Enable parameter.**

4. **Select Enable for the RIP Enable parameter.**

5. **Click on OK.**

   Site Manager displays a window that asks if the remote site is using dial optimized routing. The remote routers in this example are not using dial optimized routing.

6. **Click on Cancel.**

   You return to the RADIUS Client Configuration window.

7. **Click on Done to return to the Configuration Manager window.**

Index

A

accounting. *See* RADIUS accounting, 2-6
Acct. UDP Port parameter, A-3
alternate RADIUS servers, configuring, 2-7
Auth. UDP Port parameter, A-3
authentication
  See RADIUS, authentication, 2-3
authentication protocol. *See* PPP

B

Bay Networks Press, xv
Bay Networks World Wide Web page, xvii
Bridge Enable parameter, A-7

C

Challenge Handshake Authentication Protocol (CHAP)
  for RADIUS authentication, 2-5
client
  description, 2-1
  operating with other vendors' servers, 2-7
  router as, 2-2
  router platforms supported, 2-2
client configuration
  choosing authentication protocols, 3-3
  modifying, 3-1
  modifying the IP address, 3-1
  modifying the type of service, 3-2
  removing RADIUS authentication and accounting, 3-8
  sending server requests, 4-4
Client IP Address parameter, A-1
configuration examples
  RADIUS accounting, C-5
  RADIUS authentication, C-2
  RADIUS authentication and accounting, C-9
customer support
  programs, xvi
  Technical Solutions Centers, xvi

I

Internet drafts about RADIUS, 2-8
IP addresses
  client, 3-1
  extensions, 2-7
IP Enable parameter, A-5
IPX Enable parameter, A-6
IPXWAN Enable parameter, A-6

M

Maximum Message Retry parameter, A-3
MIB object ID, using, A-1

O

OSPF Enable parameter, A-6

P

parameters
  Acct. UDP Port, A-3
  Auth. UDP Port, A-3
  Bridge Enable, A-7

Client IP Address
defaults, B-1
IP Enable, A-5
IPX Enable, A-6
IPXWAN Enable, A-6
Maximum Message Retry, A-3
OSPF Enable, A-6
Response Timeout, A-4
RIP Enable, A-5
Server IP Address
Server Mode, A-2
Server Reset Timer, A-4
Slot Number, A-5
Password Authentication Protocol (PAP)
for RADIUS authentication, 2-5
Point-to-Point Protocol. *See* PPP
PPP
for RADIUS dial-up connections
modifying the authentication protocol, 3-6
primary server, configuring, 4-1
protocols for RADIUS authentication, 1-11, 2-3, 2-4
publications
ordering, xv

R

RADIUS
accounting
description, 2-6
protocols, 2-6
purpose, 2-6
removing, 3-8
user session, 2-6
using with dial services, 2-6
alternate servers, configuring, 4-5
authentication
choosing protocols, 3-3
description, 2-3
protocols, 2-3
removing, 3-8
UDP port setting, 4-3
Bay Networks implementation, 2-2
client, description, 2-1
configuration examples, C-2
description, 1-1, 2-1
extensions, 2-7
Internet draft specifications, 2-8
modifying the client configuration, 3-1
modifying the server configuration, 4-1
modifying the type of service, 3-2
operation with other vendors' servers, 2-7
parameters. *See* parameters
purpose, 1-1
router platforms for RADIUS, 2-2
server, description, 2-1
starting a default configuration, 1-3
Remote Authentication Dial-In User Service. *See* RADIUS
Response Timeout parameter, A-4
RIP Enable parameter, A-5
router platforms for RADIUS, 2-2

S

server
alternate, 2-7
description, 2-1
operation with other vendors' servers, 2-7
server configuration
changing the primary and alternate servers, 4-7
changing the server mode, 4-3
configuing alternate servers, 4-5
modifying the RADIUS password, 4-1
reconnecting to the primary server, 4-7
removing server entries, 4-8
requests from the client, 4-4
UDP ports, 4-3
Server IP Address parameter, A-2
Server Mode parameter, 4-3, A-2
Server Reset Timer parameter, A-4
Slot Number parameter, A-5

T

Technical Solutions Centers, xvi

U

UDP port
description, 4-3
modifying, 4-3
unnumbered circuit interfaces for authentication, 2-4

W

World Wide Web page, Bay Networks, xvii